An Inventory of International Privacy Principles: A 14 Country Analysis

Mary Francis
Dakota State University
mary.francis@dsu.edu

Quentin Covert
Dakota State University
quentin.covert@trojans.dsu.edu

Dustin Steinhagen
Dakota State University
dustin.steinhagen@trojans.dsu.edu

Kevin Streff
Dakota State University
kevin.streff@dsu.edu

Abstract

Companies are operating within a global marketplace where they must navigate differing laws related to data privacy, so it is important to understand and respect the privacy concerns of various countries. To that end, this paper will provide an inventory of the data privacy principles set out by fourteen countries around the world. By looking at the similarities and differences between nations, it is possible to work toward a common understanding and agreement of which principles should be approved and thereafter enforced. With technology evolving so rapidly, laws cannot wait to be reactionary; rather the development of privacy principles can be used to guide future implementation of regulation.

1. Introduction

2018 boasted a record number of privacy breaches [1]. The reporting of these incidents has highlighted the amount of private information that is readily collected and monetized. This use of "private" data is being challenged as public good is debated [2-4]. These discussions, however, cannot be localized as data privacy is an international issue [5-7]. The world is creating privacy methods and tools to protect privacy [8], working to integrate privacy and technology [9], and outlining key activities which must occur to keep a digital investigation private [10]. Common understanding of privacy is critical when moving forward in a world of international community.

This paper will provide a literature review looking at the understanding of privacy and the history of principles and laws related to data privacy. It will then put forth a list of overarching privacy principles. These principles will be mapped in a comparison inventory of laws of fourteen different countries and areas around the world. A discussion of the similarities and differences found within the principles will follow. Finally, suggestions for future development of data privacy principles will be provided.

2. Literature Review

Privacy has been recognized as a basic human right in numerous international agreements such as the Universal Declaration of Human Rights [11], the International Covenant on Civil and Political Rights [12], the International Covenant on Economic, Social, and Cultural Rights [13], and the American Convention on Human Rights [14]. Warren and Brandeis also discuss the importance of privacy in their seminal work *The Right to Privacy* [15].

Perhaps because of the importance of the idea, there is not a single definition of privacy [16, 17]. Rather definitions shift based on a variety of contexts including location, discipline, and era. Solove looks to "conceptualize privacy from the bottom up rather than the top down, from particular contexts rather than the abstract" [18]. Nissenbaum holds that privacy should be put into larger social contexts rather than simply "online" privacy [19]. In regards to regional differences, Diorio describes the idea of privacy in the US as based on the value of liberty from the government while privacy in the UK as the right of respect and personal dignity [20]. Westin furthers this idea on regional differences by noting "to examine how privacy norms are set in any society, we need to track three settings: the political, the socio-cultural, and the personal" [21].

Without a standard definition of privacy, there must be something that can be used to discuss the critical aspects of privacy. This is where privacy principles are so critical. A principle is a shared value upon which regulations, rules, and standards can be built for the protection and advancement of the stated objective. In Wright and Raab's in-depth discussion of privacy principles they note the importance of principles "because they form the basis for the formulation of questions that organizations can use to determine whether their new technology, system, project or policy might pose risks to one or more types of privacy" [22].

There is a long history of principles related to information privacy. One of the earliest is the US

URI: https://hdl.handle.net/10125/64276
978-0-9981331-3-3

Department of Health Education and Welfare's Fair Information Practice Principles (FIPPs) [23]. Another influential set of principles was put together and ratified by the Organization for Economic Co-operation and Development (OECD) [24]. The OECD principles continue to influence the development of privacy principles around the world which highlights how appropriate principles can withstand rapid advances in technology and cultural change.

These privacy principles are then used as the building blocks for the development of laws and regulations. One of the world's first data privacy protection laws was established in the German state of Hesse in 1970 [25]. Since that time almost 100 countries have officially enacted laws on data privacy with other laws currently under review within their assorted legislative bodies. DLA Piper has been providing an annual overview of these privacy laws since 2012 [26].

While some laws may only impact those who live within their jurisdiction, laws related to privacy of personal data or personally identifiable information must be considered more broadly. Global economics and international companies, especially within industries such as social media, have led to increasing instances where the ideas and laws related to privacy conflict across borders. Kirby, who chaired the development of the OECD Guidelines on Privacy, notes that "the growth of the impact of international law and policy on the legal discipline is the greatest change that has come upon the law" [27]. Companies such as Google, Facebook, and Twitter have come under scrutiny for their practices and have faced lawsuits for failing to comply with the laws of countries such as France, United Kingdom, and Russia. [28-31].

Prior comparisons have been done, often looking at the laws of selected countries [32, 33]. These comparisons often go in-depth into the laws looking at requirements, sanctions, and applications. [34, 35] While these comparisons provide insight into the law, these details are likely to change with the implementation of additional technologies. Privacy principles are more likely to remain constant with different changes in application.

Beyond the international lawsuits connected to privacy, there is the public push for increased privacy protections, especially as large data breaches continue to be reported. Dort and Criss provide background and future steps for businesses to consider as they move forward in this privacy landscape. [36] Hash also discusses issues for the US to consider when dealing with other nations' privacy laws [37]. Some of the consequences to business may include: damage to the organization's reputation, brand, or business relationships; possible legal or criminal liability; industry sanctions; charges of deceptive business practices; and customer and employee distrust [38]. Business and privacy are interlaced, with Calo discussing the positive relationship between the two [39]. Cavoukian's *Privacy by Design* details how privacy principles can be adopted and applied into technology systems [40]. As a basic human right, privacy must be brought to the forefront in all organizations.

3. Principles

For this comparison, one overarching list of principles has been created by which each country's principles will be mapped. In generating this list of overarching principles, several lists of principles, including those in the laws themselves were consulted. Some of these included: Fair Information Practice Principles [23], OECD [24], Generally Accepted Privacy Principles, [38], and OASIS's Privacy Management Reference Model and Methodology [41].

Descriptions of each principle are included below. Since a country may enumerate various ideas under a single principle, it is possible for a country to have more principles on the overarching list than the number they provide within their own laws and standards. An attempt was made in creating the list of principles to break each concept into a single definitive item - while the combination of ideas may be natural in one context it will not fit within another. Each principle listed in the laws was analyzed to consider whether the concept fit within a previous principle or whether the idea was novel enough to add new principles to the overarching list.

When looking at the descriptions of each principle within the various laws, the underlying meaning was delved in order to assign one of the overall principles listed below. The broad expansiveness of language, especially with translations of different languages, requires a consolidation of ideas. This focus on the language and definition of the principles is important as "Regulatory law and practice ideally depend upon precision in the expression and elaboration of principles and the guidelines, codes of practice and other instruments that constitute implementation. Given the globalization of information processing, consistency in the enunciation of principles and perforce in their legal embodiment and practical interpretation has been seen as important, although concrete variations are tolerable as long as the underlying principles are reasonably uniform" [22].

Overall, twenty-one separate privacy principles were included in the inventory. Some principles were addressed in all the laws considered and others were only found in a single law. While this listing is not meant

to be comprehensive of all data privacy principles, it does provide a more in-depth consideration of data privacy principles than is found in any single compilation.

Notice: Subjects will be informed of data collection and use policies

Retention: Data will be removed when no longer required

Minimization: Limit the amount of data collected, processed, and stored

Use restriction: Data can only be used for defined and accepted purposes

Security: Data is handled in accordance with appropriate security principles

Quality: Data is accurate and kept up to date

Access: Subjects have the right to know what personal data is being held about them

Participation: Allow data to be corrected and deleted by the subjects of the data whenever appropriate

Enforcement: Data holders must comply with applicable policies, laws, and standards

Consolidation: Consolidation of databases containing personal data cannot be done

Consent: Enable data subjects to agree to data collection

Transparency: Make all data collection, use, storage, and deletion as transparent as possible with clear and understandable language used to explain all privacy-related policies

Context: Apply the context of the jurisdiction one operates in into privacy policies

Accountability: Privacy policies must be developed that clearly describe the practices and procedures related to the management of personal data

Identifiability: Data subjects have the option of remaining anonymous or using a pseudonym

Sensitivity: Treat all data collected, used, stored, and destroyed in manners appropriate to the sensitivity level of the data

Information flow: Enable the communication of personal information across multiple contexts, including international, governmental, economic, and social

Identifiers: Strong identifiers are only used when necessary

Disclosure: Make known any data transference to new parties

Confidentiality: Maintain confidentiality of data throughout processes and beyond

Breach: Subjects must be informed immediately of any data breach involving their personal data

4. Methods

Several criteria were considered in selecting the countries to include in this analysis. First, the country had to have a current law, regulation, act, etc. related to the privacy of individuals' data. Second, the full law had to be available for analysis in English. Finally, effort was made to select a range of countries representing areas around the world. There is one instance where the privacy principles were not contained in the language of the law itself. China passed the PRC Cybersecurity Law from which several standards provide additional details on implementation. The Information Security Technology – Personal Information Security Specifications provide the privacy principles.

When conducting the analysis, only the principles section of the law was reviewed. It is possible that concepts described in other overarching principles may be found within remaining sections of the law. However, this analysis focused solely on those items that each country deemed important enough to describe within a dedicated principles section.

The analysis section below will include: the country or area overseen by the law, the name of the law, the year which the law was enacted, a listing of the privacy principles as stated in the law followed by the overarching principles addressed by that principle in parenthesis, and a list of the overarching principles referenced within the law. Most of the laws will contain a mapping in parenthesis of the overarching principles connected to a specific principle. Ghana, Mexico, and the Philippines will not have a direct mapping as their description of each principle is not connected to the principle itself.

5. Analysis

Table 1. Laws included in analysis

Country / Region	Law	Section reviewed for analysis
Australia	Privacy Act 1988	Schedule 1
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	Schedule 1
China	PRC Cybersecurity Law Privacy information contained in the standard Information Security	Section 4

	Technology – Personal Information Security Specifications	
Colombia	Statutory Law 1266	Article 4
European Union	General Data Protection Regulation (GDPR) Regulation (EU) 2016/678	Chapter II Article 5
Ghana	Data Protection Act, 2012 (Act 843)	Section 17 – Section 34
Hong Kong	Personal Data (Privacy) Ordinance (Cap. 486)	Schedule 1
Malaysia	Personal Data Protection Act 2010	Part II Section 5 – Section 12
Mexico	Federal Law on the Protection of Personal Data held by Private Parties	Chapter II Article 6 – Article 21
New Zealand	Privacy Act 1993	Part 2 Section 6
Philippines	Data Privacy Act of 2012 or Republic Act No. 10173	Chapter III Section 11
Russia	Data Protection Act No. 152 FZ	Chapter 2 Article 5
South Africa	Protection of Personal Information Act 4 of 2013	Chapter 3 Article 8 – Article 25

Australia - *Privacy Act 1988*, 2018 "An Act to make provision to protect the privacy of individuals, and for related purposes." [42]

- open and transparent management of personal information (accountability and transparency)
- anonymity and pseudonymity (identifiability)
- collection of solicited personal information (minimization and consent)
- dealing with unsolicited personal information (retention)
- notification of the collection of personal information (notice)
- use or disclosure of personal information (use restriction and disclosure)
- direct marketing (use restriction)
- cross-border disclosure of personal information (information flow)
- adoption, use or disclosure of government related identifiers (identifiers)
- quality of personal information (quality)
- security of personal information (security)
- access to personal information (access)
- correction of personal information (participation)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, access, consent, participation, transparency, disclosure, accountability, identifiability, information flow, and identifiers.

Brazil - *General Data Protection Law No. 13,709*, 2018

"This Law provides for the processing of personal data, including by digital means, by a natural person or a legal entity of public or private law, with the purpose of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person." [43]

- Purpose (use restriction and notice)
- Suitability (use restriction)
- Necessity (minimization)
- Free access (access and participation)
- Quality of the data (quality)
- Transparency (transparency)
- Security (security)
- Prevention (security)
- Nondiscrimination (enforcement)
- Accountability (enforcement)

These principles fall under the overarching principles: notice, minimization, use restriction, security, quality, access, enforcement, participation, and transparency.

Canada - *Personal Information Protection and Electronic Documents Act (PIPEDA)*, 2000

"An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act." [44]

- Accountability (enforcement and accountability)
- Identifying purposes (notice, disclosure, use restriction, and transparency)
- Consent (consent, use restriction, sensitivity, and transparency)
- Limiting collection (minimization)

- Limiting use, disclosure, and retention (use restriction, retention, and disclosure)
- Accuracy (quality)
- Safeguards (security and sensitivity)
- Openness (notice and transparency)
- Individual access (access and participation)
- Challenging compliance (enforcement)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, access, enforcement, consent, participation, transparency, disclosure, accountability, and sensitivity.

China - *Information security technology – Personal information security specifications,* 2018

"These standards specifies [*sic*] the principles and security requirements that should be followed in acts handling personal information such as collection, storage, use, sharing, transfer, and disclosure.

This standard is applied to regulate all types of organizations' activities handling personal information, and is also applied to the competent supervisory departments and third-party assessment organizations supervision, management and evaluation of personal information handling activities." [45]

- Commensurate powers and responsibilities (enforcement)
- Clear purpose (use restriction)
- Choice and consent: (notice and consent)
- Minimum sufficient use (minimization and retention)
- Openness and transparency (transparency)
- Ensuring security (security)
- Subject participation (access and participation)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, access, enforcement, consent, participation, and transparency.

Colombia - *Statutory Law 1266,* 2008

"This law aims to develop the constitutional right of all people to know, update and rectify information gathered about them in databases, and other rights, freedoms and constitutional guarantees related to the collection, treatment and movement of personal that Article 15 of the Constitution refers to data and the right to information provided for in Article 20 of the Constitution, particularly in relation to the financial and credit, business information, services and from third countries." [46]

- Accuracy or quality of the records of data (quality)
- Finality (notice, consent, and enforcement)
- Restricted circulation (enforcement, use restriction)
- Timeliness of information (use restriction)
- Comprehensive interpretation of constitutional rights (enforcement)
- Security (security)
- Confidentiality (confidentiality)

These principles fall under the overarching principles: notice, use restriction, security, quality, enforcement, consent, and confidentiality.

European Union - *General Data Protection Regulation (GDPR) Regulation (EU) 2016/678,* 2016

"On the protection of natural persons with regard to the processing of personal data and on the free movement of such data"[47]

- Lawfulness, fairness and transparency (enforcement and transparency)
- Purpose limitations (use restriction and notice)
- Data minimization (minimization)
- Accuracy (quality)
- Storage limitations (retention)
- Integrity and confidentiality (security)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, enforcement, and transparency.

Ghana - *Data Protection Act,* 2012

"An Act to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use, or disclose personal information and for related matters." [48]

- Accountability
- Lawfulness of processing
- Specification of purpose
- Compatibility of further processing with purpose of collection
- Quality of information
- Openness
- Data security safeguards
- Data subject participation

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, access, enforcement, consent, participation, transparency, disclosure, breach, and context.

Hong Kong - *Personal Data (Privacy) Ordinance Cap. 486,* 2018

"An Ordinance to protect the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith." [49]

- Purpose and manner of collection of personal data (minimization, use restriction, enforcement, notice, and consent)
- Accuracy and duration of retention of personal data (quality and retention)
- Use of personal data (disclosure)
- Security of personal data (security)
- Information to be generally available (notice and transparency)
- Access to personal data (access and participation)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, access, enforcement, consent, participation, transparency, and disclosure.

Malaysia - *Personal Data Protection Act*, 2010

"An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto." [50]

- General Principle (consent, use restriction, and minimization)
- Notice and Choice Principle (notice, access, participation, disclosure, and transparency)
- Disclosure Principle (use restriction and disclosure)
- Security Principle (security)
- Retention Principle (retention)
- Data Integrity Principle (quality)
- Access Principle (access and participation)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, access, consent, participation, transparency, and disclosure.

Mexico - *Federal Law on Protection of Personal Data Held by Private Parties*, 2010

"This Law is of a public order and of general observance throughout the Republic, and has the purpose of protecting personal data held by private parties, in order to regulate its legitimate, controlled and informed processing, to ensure the privacy and the right to informational self-determination of individuals." [51]

- Legality
- Consent
- Notice
- Quality
- Purpose
- Fidelity
- Proportionality
- Accountability

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, access, enforcement, consent, participation, transparency, disclosure, breach, confidentiality, and sensitivity.

New Zealand - *Privacy Act*, 1993

"An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data…" [52]

- Purpose of collection of personal information (use restriction and enforcement)
- Source of personal information (consent)
- Collection of information from subject (notice)
- Manner of collection of personal information (consent and enforcement)
- Storage and security of personal information (security)
- Access to personal information (access and participation)
- Correction of personal information (participation)
- Accuracy, etc, of personal information to be checked before use (quality)
- Agency not to keep personal information for longer than necessary (retention)
- Limits on use of personal information (use restriction)
- Limits on disclosure of personal information (disclosure)
- Unique identifiers (identifiers)

These principles fall under the overarching principles: notice, retention, use restriction, security, quality, access, enforcement, consent, participation, disclosure, and identifiers.

Philippines - *Republic Act 10173 – Data Privacy Act of* 2012, 2012

"An Act protecting individual personal information in information and communications systems in the government and the private sector, creating for this purpose a national privacy commission, and for other purposes." [53]

- Transparency
- Legitimate purpose
- Proportionality

These principles fall under the overarching principles: notice, retention, minimization, use restriction, quality, and enforcement.

Russia - *Federal Law No. 152-FZ Personal Data*, 2006

"This Federal Law regulates the relations connected with personal data processing carried out by federal state authorities, state authorities of Russian Federation constituents, other state bodies (hereinafter – state bodies), legal entities, natural individuals with the help of automation aids or without them if personal data processing without such aids corresponds to the nature of actions (operations) done with personal data with the help of automation aids." [54]

- legality of the purposes and methods of personal data processing and good faith (enforcement)
- correspondence of the purposes of personal data processing to the purposes determined earlier and stated during personal data gathering, also to the operator's authority (notice)
- correspondence of the volume and nature of the processed personal data, personal data processing techniques to the purposes of personal data processing (use restriction)
- personal data reliability, their sufficiency for the processing purposes, inadmissibility of processing personal data that are excessive relative to the purposes stated during personal data gathering (quality and minimization)
- inadmissibility of integration of databases of personal data information systems, created for inter-incompatible purposes (consolidation)
- Personal data storage should be done in a form allowing identification of the personal data subject for not longer than required for the purposes of their processing, and they are to be destroyed upon attainment of the processing purposes or in case their attainment becomes unnecessary (retention)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, quality, enforcement, and consolidation.

South Africa - *No. 4 of 2013: Protection of Personal Information Act*, 2013

"To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith." [55]

- Accountability (enforcement)
- Processing limitation (enforcement, minimization, use restriction, and consent)
- Purpose specification (use restriction, notice, and retention)
- Further processing limitation (disclosure)
- Information quality (quality)
- Openness (transparency and notice)
- Security (security and breach)
- Data subject participation (access and participation)

These principles fall under the overarching principles: notice, retention, minimization, use restriction, security, quality, access, enforcement, consent, participation, transparency, disclosure, and breach.

Table 2. Data privacy principles addressed by country

	Australia	Brazil	Canada	China	Colombia	European Union	Ghana
Notice	X	X	X	X	X	X	X
Retention	X		X	X		X	X
Minimization	X	X	X	X		X	X
Use Restrict	X	X	X	X	X	X	X
Security	X	X	X	X	X	X	X
Quality	X	X	X		X	X	X
Access	X	X	X	X			X
Enforcement		X	X	X	X	X	X
Consent	X		X	X	X		X
Participation	X	X	X	X			X
Transparency	X	X	X	X		X	X
Disclosure	X		X				X
Accountability	X		X				
Breach							X
Confidentiality					X		
Consolidation							
Identifiability	X						
Sensitivity			X				
Context							X

Info Flow	X						
Identifiers	X						

	Hong Kong	Malaysia	Mexico	New Zealand	Philippines	Russia	South Africa
Notice	X	X	X	X	X	X	X
Retention	X	X	X	X	X	X	X
Minimization	X	X	X		X	X	X
Use Restrict	X	X	X	X	X	X	X
Security	X	X	X	X			X
Quality	X	X	X	X	X	X	X
Access	X	X	X	X			X
Enforcement	X		X	X	X	X	X
Consent	X	X	X	X			X
Participation	X	X	X	X			X
Transparency	X	X	X				X
Disclosure	X	X	X	X			X
Accountability							
Breach			X				X
Confidentiality			X				
Consolidation						X	
Identifiability							
Sensitivity			X				
Context							
Info Flow							
Identifiers				X			

6. Discussion

An inventory of 14 laws were mapped onto a listing of 21 data privacy principles. The countries addressing the largest number of principles were Australia and Mexico with 15 principles each. The Philippines addressed the fewest principles with 6. Across the 14 laws, the average number of principles addressed was 10.8.

There were two principles that were found in each law, notice and use restriction. Other frequently occurring principles include: quality (13 laws), retention (12), minimization (12), security (12), enforcement (12), access (10), consent (10), participation (10), transparency (10), and disclosure (8). There were four principles that each only appeared in the law of one country: information flow, context, identifiability, and consolidation. Other infrequent principles were sensitivity (2), confidentiality (2), breach (3), and accountability (2).

In considering the principles there are some that make complementary partners and others whose descriptions may result in their combination. Access and participation both deal with the subjects' rights relating to their data. While access allows the individual to see the personal data that is held on them, participation allows them to request corrections or deletion of that data. It would be possible to allow access without participation, but each law that allowed access also provided the right of participation. Sensitivity and context are principles that also have a strong relationship. Sensitivity requires data to be handled differently depending on its sensitivity level which often is determined by the context of the data processing. Confidentiality is also related to security in that it may be considered a subset of proper security protocols.

The designation of enforcement was made when the principles included language relating to how the data controller, organization, etc. had to comply with laws, regulations, or other statutes. Enforcement could also be applied in principles that discussed "lawful purpose" or "legal purpose" in relation to data collection. A related principle is accountability. Accountability holds that the organization must develop privacy policies while enforcement ensures compliance with those policies. Accountability does not occur frequently as a principle; however, it may be that accountability is subsumed under the principle of transparency which notes that polices must be understandable to data subjects.

Breach is a principle that was not found in other listings of privacy principles, yet it is mentioned by three of the countries. It involves an additional action on the part of the data holder by requiring notification of data subjects of any data breach, allowing them the opportunity to counteract any possible harms. This principle would be applied if there was a break in security and is found in those countries that also have the related principles of transparency, disclosure, and notice.

The principle of identifiers has been assigned to countries that specifically discuss assigning strong identifiers to data subjects. This is in relation to avoiding the use of governmental IDs when they are not necessary to help maintain privacy. Another example of a strong identifier would include biometric data. A related principle is identifiability which provides individuals the right to remain anonymous or use pseudonyms.

Each law is introduced with language describing its purpose. There are several trends that appear in these descriptions. First, countries describe how they are regulating information or creating a commission to oversee the data (Ghana, Malaysia, Mexico, New Zealand, Philippines, Russia, and South Africa). Given the fact that these are laws, this focus on rules is not surprising. Other countries provide an economic reason for the law by noting how commerce is affected (Canada, Colombia, and Malaysia). Process is another concept that is discussed (Brazil, China, European

Union, Ghana, Malaysia, and South Africa). The most frequently addressed idea is protection of privacy (Australia, Brazil, Canada, European Union, Ghana, Hong Kong, Mexico, New Zealand, Philippines, and South Africa). Here it is the individual who is given focus. Brazil and Mexico actually include language that goes beyond simple protection of the individual to the "free development of the personality of the natural person" [43] and "the right to informational self-determination of individuals" [51].

7. Conclusion

Privacy is a basic human right and it is held to a high standard by individuals and thereby the countries they reside within. While the specific context and degree of data privacy may vary, there remains a constant belief that privacy must be protected by law, policies, and procedures. As the global community becomes more interconnected, clashes around differing privacy cultures are inevitable. It is important to understand what privacy means across the world.

When considering which data privacy principles may be the most important to address in any standards or procedures, the twelve that occur the most frequently include: notice, use restriction, quality, retention, minimization, security, enforcement, access, consent, participation, transparency, and disclosure. Those that occur infrequently include: information flow, context, identifiability, consolidation, sensitivity, confidentiality, breach, and accountability. The specific application of data privacy principles will vary given the context and goals of an individual country, jurisdiction, industry, or organization. However, by basing these applications upon an agreed acceptance of principles, the privacy rights of the individual will be acknowledged.

Future work on this topic would analyze each of the privacy principles in depth to ensure consistency in use across the laws. This analysis could also provide descriptions of the principles for international understanding and acceptance.

8. References

[1] C. Landwher, "Privacy and Security 2018: A Big Year for Privacy," (in English), *Association for Computing Machinery. Communications of the ACM*, vol. 62, no. 2, p. 20, Feb 2019.

[2] A. Blaszczak-Boxe. (2019, Jan 2019) Facial Recall: App for identifying faces raises privacy concerns. *Scientific American*. 18.

[3] D. Jeske and K. S. Shultz, "Social media screening and content effects: implications for job applicant reactions," (in English), *International Journal of Manpower*, vol. 40, no. 1, pp. 73-86, 2019.

[4] G. Tett, "Privacy concerns collide with the public interest in data [Europe Region]," in *Financial Times*, ed. London (UK), 2019, p. 9.

[5] S. Agarwal and D. Sengupta, "FB breach: Privacy advocates in India seek stronger data laws [Internet]," in *The Economic Times*, ed. New Delhi, 2018.

[6] C. Stupp, "European Privacy Regulators Find Their Workload Expands Along With Authority; Facing prospect of steep fines, companies report minor breaches beyond scope of GDPR," (in English), *WSJ Pro. Cyber Security*, 2019 Apr 12.

[7] J. Williams, "Panelists Offer Views on Data Privacy Legislation," (in English), *Cybersecurity Policy Report*, p. 1, 2019 Feb 11.

[8] Y.-S. Martin and A. Kung, "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering," presented at the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2018.

[9] A. Sokolovska and L. Kocarev, "Integrating Technical and Legal Concepts of Privacy " *IEEE Journals & Magazines* vol. 6, pp. 26543 - 26557, 2018.

[10] A. Dehghantanha and K. Franke, "Privacy-respecting digital investigation " presented at the 2014 Twelfth Annual International Conference on Privacy, Security and Trust 2014.

[11] (1948). *The Universal Declaration of Human Rights*.

[12] (1966). *International Covenant on Civil and Political Rights* [Online] Available: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

[13] (1966). *International Covenant on Economic, Social, and Cultural Rights*. [Online] Available: International Covenant on Economic, Social, and Cultural Rights

[14] (1969). *American Convention on Human Rights*. [Online] Available: https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm

[15] S. D. Warren and L. D. Brandeis, "The Right to Privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193-220, 1890.

[16] C. Castelli. (2014) Privacy Engineering Concepts Avoid Defining Privacy. *Inside Cybersecurity*.

[17] T. Weimann and D. Nagel, "Agreeing on a Definition for Data Protection in a Globalized World," *IEEE Technology and Society Magazine* vol. 31, no. 4, pp. 39-42, 2012.

[18] D. Solove, "Conceptualizing Privacy," *California Law Review*, Article vol. 90, no. 4, p. 1088, 2002.

[19] H. Nissenbaum, "Contextual Approach to Privacy Online," *Dædalus*, vol. 140, no. 4, pp. 32-48, 2011.

[20] S. Diorio, "Data Protection laws: Quilts versus blankets," *Syracuse Journal of International Law & Commerce*, Article vol. 42, no. 2, pp. 485-513, Spring2015 2015.

[21] A. Westin, "Social and Political Dimensions of Privacy," *Journal of social issues*, vol. 59, no. 2, pp. 431-453, 2003.
[22] D. Wright and C. Raab, "Privacy principles, risks and harms," *International Review of Law, Computers & Technology*, vol. 28, no. 3, pp. 277-298, 2014.
[23] (1973). *Code of Fair Information Practices*.
[24] (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. [Online] Available: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[25] F. H. Cate, "The EU Data Protection Directive Information Privacy and the Public Interest," *Iowa Law Review*, vol. 80, pp. 431-443, 1995.
[26] D. Piper. (2019). *Data Protection Laws of the World* [Online]. Available: https://www.dlapiperdataprotection.com/.
[27] M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy," *International Data Privacy Law*, vol. 1, no. 1, pp. 6-14, 2011.
[28] T. R. Weiss, "Google Faces Imminent French Sanctions on User Privacy Issues," *eWeek*, Article pp. 2-2, 2013.
[29] T. Geller, "In Privacy Law, It's the U.S. vs. the World," *Communications of the ACM*, Article vol. 59, no. 2, pp. 21-23, 2016.
[30] H. Leung, "U.K. Lawmakers Accuse Facebook of 'Intentionally and Knowingly' Violating Data Privacy Laws and Call for Stricter Regulation," *Time.com*, 2019.
[31] A. M. Simmons, "Russia Accuses Facebook, Twitter of Failing to Comply With Data Laws," *Wall Street Journal - Online Edition*, Article p. 1, 2019.
[32] G. Greenleaf and P. Whon-il, "South Korea's innovations in data privacy principles: Asian comparisons," *Computer Law & Security Review*, Article vol. 30, no. 5, pp. 492-505, 2014.
[33] G. E. Kennedy and L. S. P. Prabhu, *Data Privacy Law: A Practical Guide 2nd Edition*. 2017.
[34] I. A. o. P. Professionals. (2019). *The General Data Protection Regulation Matchup Series* [Online]. Available: https://iapp.org/resources/article/the-general-data-protection-regulation-matchup-series/.
[35] C. Rich, "Privacy Laws in East, Central and South Asia andthe Pacific," *World Data Protection Report*, 2016.
[36] K. K. Dort and J. T. Criss, "Trends in Cybersecurity Law, the Privacy Shield, and Best Practices for Businesses Operating in the Global Marketplace," *Computer & Internet Lawyer*, Article vol. 33, no. 7, pp. 3-10, 2016.
[37] R. Hash, "Fundamental Differences in Privacy Laws can Undermine Economic Ties and Multinational Corporate Plans: What Companies can do to Prepare for the Next Safe Harbor Moment," *North Carolina Journal of International Law & Commercial Regulation*, Article vol. 42, no. 4, pp. 1061-1093, Summer2017 2017.
[38] D. Schroeder and N. A. Cohen, "GAPP Targets PRIVACY Risks," *Journal of Accountancy*, Article vol. 212, no. 1, pp. 52-56, 2011.
[39] R. Calo, "Privacy and Markets: A Love Story," *Notre Dame Law Review*, vol. 91, no. 2, 2016.
[40] A. Cavoukian, "Privacy by design: The 7 foundational principles," *Information and Privacy Commissioner of Ontario, Canada*, 2009.
[41] "Privacy Management Reference Model and Methodology (PMRM) Version 1.0," OASIS Committee Specification 02, 2016, [Online]. Available: http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html#_Toc452024302.
[42] "Privacy Act 1988," ed. Australia, 2018.
[43] "General Data Protection Law No. 13,709," ed. Brazil, 2018.
[44] "Personal Information Protection and Electronic Documents Act," ed. Canada, 2018.
[45] "Information security technology—Personal Information Security Specifications," ed. China: National Standardization Administration 2018.
[46] "Statutory Law 1266," ed. Colombia, 2008.
[47] "General Data Protection Regulation (GDPR) Regulation (EU) 2016/678," ed. European Union, 2016.
[48] "Data Protection Act," ed. Ghana, 2012.
[49] "Personal Data (Privacy) Ordinance," ed. Hong Kong, 2018.
[50] "Personal Data Protection Act 2010," ed. Malaysia, 2010.
[51] "Federal Law on Protection of Personal Data Held by Private Parties," ed. Mexico, 2010.
[52] "Privacy Act 1993," ed. New Zealand, 1993.
[53] "Data Privacy Act of 2012," ed. Philippines, 2012.
[54] "Personal Data," ed. Russia, 2006.
[55] "Protection of Personal Information Act," ed. South Africa, 2013.